DOI: 10.58168/MoInSyTe2024_358-364
УДК 004.9

# АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРСОНАЛЬНЫХ НОСИМЫХ УСТРОЙСТВ

В.И. Анциферова[1], А.С. Фролов[1], В.С. Шапкин[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В работе рассматриваются принципы работы и основы Wi-Fi сетей, их безопасность и средства защиты.

Ключевые слова: Wi-Fi, беспроводные сети, безопасность, протокол безопасности, хакерские атаки.

# SECURITY ANALYSIS OF WIRELESS NETWORKS OF PERSONAL WEARABLE DEVICES

V.I. Antsiferova[1], A.S. Frolov[1], V.S. Shapkin[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The paper discusses the principles of operation and fundamentals of Wi-Fi networks, their security and means of protection.

Keywords: Wi-Fi, wireless networks, security, security protocol, hacker attacks.

В современном мире беспроводные технологии обмена информацией на основе стандартов IEEE 802.11 заняли очень важное место. Беспроводные сети – это сети радиосвязи, которые удобны в использовании, имеют неплохую пропускную способность и относительно недорогие для общественного пользования. Подключение персональных устройств к сети Ethernet все реже происходит с помощью кабеля, но вместе с этим повышаются требования к защите информации в беспроводных сетях.

Международные хакерские группировки, такие, как Anonymous, кибер вымогатели Conti и другие активно пытаются внедряться в важнейшие Российские

ресурсы и нарушать их работоспособность. Например, 9 мая 2022 года была проведена мощнейшая APT- атака на видео хостинг “Rutube”, в результате чего доступ к сервису был потерян почти на день. Хакеры влезли в систему, модифицировали код так, чтобы он удалял данные сервиса из хранилища. Конечно, простые люди не являются целью этих группировок, однако, и на территории нашей страны немало мелких бандитских групп, занимающихся взломом, кражей денег и информации у простых людей. Примерно половина атак и взломов происходит по слабо защищенным Wi-Fi сетям и каналам. Именно поэтому тема кибер безопасности и безопасности Wi-Fi сетей крайне важна, и каждый человек должен надежно защищать свои персональные устройства и данные.

Стандарты работы Wi-Fi. Рассмотрим работу сети на примере подключения к интернету в квартире. Через сетевой интернет-кабель роутер получает трафик, преобразовывает его в радиоволны и транслирует в виде радиосигналов.

Приемник, коим может являться компьютер, ноутбук, планшет, смартфон, ТВ, видит эти волны, принимает и декодирует их.

Характеристики стандарта. За все годы развития технологии было множество вариаций и версий стандарта. Рассмотрим основные стандарты Wi-Fi 802.11 (рис. 1).

| Протокол | Тактовая частота | Ширина канала | MIMO | Макс. скорость передачи данных (теоретическая) |
|---|---|---|---|---|
| 802.11ax | 2,4 или 5 ГГц | 20, 40, 80, 160 МГц | Многопользовательский (MU-MIMO) | 2,4 Гбит/с[1] |
| 802.11ac wave2 | 5 ГГц | 20, 40, 80, 160 МГц | Многопользовательский (MU-MIMO) | 1,73 Гбит/с[2] |
| 802.11ac wave1 | 5 ГГц | 20, 40, 80 МГц | Однопользовательский (MIMO SU) | 866,7 Мбит/с[2] |
| 802.11n | 2,4 или 5 ГГц | 20, 40 МГц | Однопользовательский (MIMO SU) | 450 Мбит/с[3] |
| 802,11g | 2,4 ГГц | 20 МГц | Н/Д | 54 Мбит/с |
| 802.11a | 5 ГГц | 20 МГц | Н/Д | 54 Мбит/с |
| стандарт 802.11b | 2,4 ГГц | 20 МГц | Н/Д | 11 Мбит/с |
| Устаревший версии 802.11 | 2,4 ГГц | 20 МГц | Н/Д | 2 Мбит/с |

Рисунок 1 – Стандарты Wi-Fi

По спецификации 802.11a данные передаются со скоростью до 54 Мбит/с в секунду. Он предусматривает также мультиплексирование с ортогональным делением частот (orthogonal frequency-division multiplexing OFDM), более эффективную технику кодирования, предусматривающую разделение исходного сигнала на передающей стороне на несколько подсигналов. Такой подход

позволяет уменьшить воздействие помех. Радиус работы (дальность) в помещении – 35 м.

Спецификация 802.11b является самой медленной и наименее дорогой. На некоторое время, благодаря своей стоимости, она получила широкое распространение, но сейчас была вытеснена. Стандарт 802.11b предназначен для работы в диапазоне 2,4 ГГц. Скорость передачи данных составляет до 11 Мбит/с в секунду при использовании для повышения скорости манипуляции с дополняющим кодом. Радиус работы (дальность) в помещении – 38 м.

Спецификация 802.11g, как и 802.11b, предусматривает работу в диапазоне 2,4 ГГц, однако обеспечивает значительно большую скорость передачи данных - до 54 Мбит/с в секунду. Стоит заметить, что диапазон 2.4 ГГц не является лицензированным. Спецификация 802.11g быстрее, поскольку в ней используется такое же кодирование, как и в 802.11a. Радиус работы (дальность) в помещении – 38 м.

Самая широко распространенная спецификация - 802.11n. В ней существенно увеличена скорость передачи данных и расширен частотный диапазон. Спецификация 802.11n может обеспечить скорость передачи данных 140 Мбит/с в секунду, в идеальных условиях. Радиус работы (дальность) в помещении – 70 м.

IEEE 802.11ac — спецификация, работающая в диапазоне частот 5 ГГц, получила название Wi-Fi 5. Позволяет существенно расширить пропускную способность сети, начиная от 433 Мбит/с и до 6,77 Гбит/с. Это наиболее существенное нововведение относительно IEEE 802.11n. Кроме того, ожидается снижение энергопотребления (Дж/бит), благодаря чему увеличится время автономной работы мобильных устройств. В 2020 гг. заменена спецификацией IEEE 802.11ax (Wi-Fi 6). Радиус работы (дальность) в помещении – 112 м.

Wi-Fi 6 - спецификация беспроводных локальных компьютерных сетей в наборе стандарта IEEE 802.11. В дополнение к использованию технологий MIMO, в стандарте WiFi 6 вводится режим ортогонального частотного мультиплексирования для улучшения спектральной эффективности, и модуляция для увеличения пропускной способности; хотя номинальная скорость передачи данных только на 37 % выше, чем в предыдущем стандарте IEEE 802.11ac, ожидается, что Wi-Fi 6 позволит в 4 раза увеличить среднюю пропускную способность. Устройства данного стандарта предназначены для работы в уже существующих диапазонах 2,4 ГГц и 5 ГГц, но могут включать дополнительные полосы частот в диапазонах от 1 до 7 ГГц.

802.11ad – самая быстрая, на данный момент, технология Wi-Fi, имеющая неофициальное название WiGig. Способна передавать данные со скоростью до 7 Гбит/с, однако сигнал действует только примерно на расстоянии до 10 метров. И передавать данные можно только в зоне прямой видимости. Именно поэтому 802.11ad не используется в беспроводных роутерах.

Возникающие при работе Wi-Fi сетей угрозы можно разделить на два типа:

- Прямые угрозы – возникают при передаче информации по беспроводному интерфейсу 802.11;
- Косвенные угрозы – связанные с наличием на объекте или рядом с объектом большого количества Wi-Fi сетей.

За последние несколько лет человечество наблюдало сильные вирусные атаки, такие как, например, Expetya и Wannacry, что говорит о наличии уязвимостей в информационной безопасности как домашних Wi-Fi сетей, так и больших корпоративных сетей. Хакеры, создатели вредоносных программ после создания ПО многократно тестируют и проверяют свой “продукт” на обнаружение популярными антивирусными программами и это дает плоды. Только через несколько часов хороший антивирус распознает угрозы и пополняет базу. Слабые “защитники” могут вовсе не успеть увидеть врага и будут сами заражены.

Самыми популярными угрозами являются:

- ботнеты;
- атаки на веб-приложения;
- шифровальщики;
- целевые атаки;
- фишинг;
- уязвимости в ОС;
- уязвимости в устанавливаемом ПО;
- нецелевые атаки.

Конечно, простые межсетевые экраны и средства защиты, изобретенные в далеких 2000х годах, можно забыть. Позже на их смену пришли многофункциональные интернет-шлюзы (MSBG), которые имеют неплохой функционал. И да, этот же обширный функционал используется хакерами, как разнообразие для выбора атакуемой цели. Сейчас же для защиты сетевого периметра используются современные шлюзы безопасности (UTM) (рис. 2) и усовершенствованные межсетевые экраны (NGFW) (рис. 3).

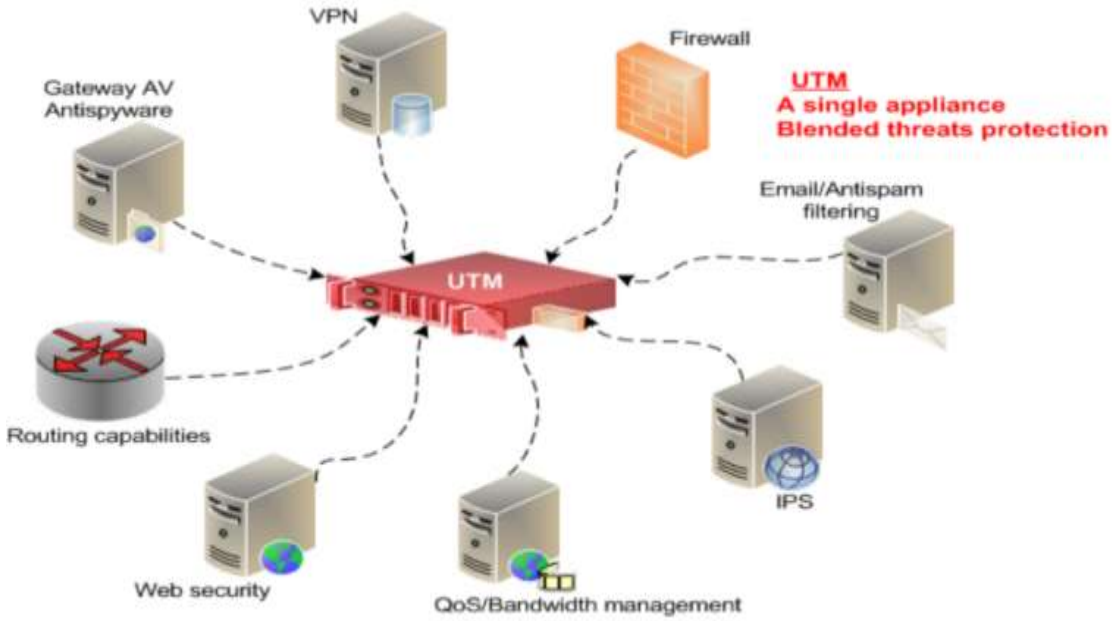


Рисунок 2 – Unified Threat Management

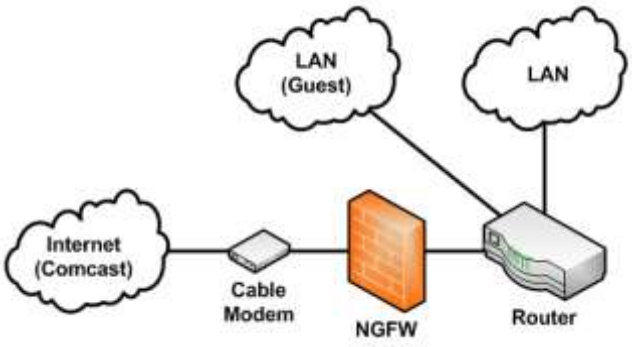


Рисунок 3 – Next-Generation Firewall

Отличие этих типов решений в наличии систем глубокого анализа входящего и выходящего трафика. Происходит анализ ошибок сетевых протоколов, характер сетевых соединений, обращения к подозрительным ресурсам и выявляются угрозы в обычном типе трафика.На каждом этапе развития беспроводных технологий росла и их защита. Внедрение и применение технологии TKIP (Протокол целостности временного ключа в протоколе защищённого беспроводного доступа Wi-Fi Protected Access) добавило к базовому шифрованию WEP немало функций, таких, как:

- TimeStamp – добавление метки времени в алгоритм шифрования MIC

- Счетчик последовательностей TKIP, который обеспечивает запись кадров, отправленных по уникальному MAC-адресу для предотвращения использования атаки методом повторения кадров

- Алгоритм смешивания ключей, который вычисляет для каждого кадра уникальный 128-битный ключ

Однако, TKIP был крайне уязвимым и на его замену пришел более безопасный Counter/CBC-MAC (CCMP), состоящий из двух алгоритмов

- CBC-MAC – для проверки целостности сообщений MIC

- AES шифрование в режиме счетчика

Никакие методы шифрования не спасут без установления подлинности и подтверждения запроса пользователя для подключения к сети, то есть без аутентификации. Только после выполнения аутентификации пользователь получает доступ к сети по безопасным каналам. Существуют следующие методы аутентификации:

Открытая. Защита сети на основе ограничения доступа, что не является безопасным способом. В запросе аутентификации присутствует только MAC – адрес.Используется статический WEP и CKIP

Аутентификация с общим ключом. Пользователь делает запрос на аутентификацию, в ответ получает подтверждение, содержащее 128 байт информации. Далее происходит WEP шифрование и тест отправляется точке доступа на расшифровку. В случае совпадения текста пользователь подключается к сети. Весьма уязвимая схема аутентификации, на нее проводятся атаки “Maninthemiddle”.Используется шифрование CKIP и динамический WEP.

Аутентификация по MAC – адресу. Метод поддерживается производителем Cisco и D-Link, однако в 802.11 не предусмотрен. MAC адрес сравнивается с таблицей разрешенных адресов и используется как дополнительная мера защиты.

- WPA. Промежуточный стандарт, включающий в себя новую систему аутентификации с помощью RADIUS сервера и предустановленного ключа WPA-PSK.Используется шифрование TKIP, расширение AES-CCMP, в качестве обратной совместимости WEP.

- WPA2. Довольно безопасный метод, в качестве шифра выбран блочный AES. Так же, как и в WPA, предусмотрено два варианта аутентификации.

- WPA3. В нем алгоритм TKIP/AES был заменен на шифрование SAE, также были устранены уязвимости, способствующие атакам KRACK. Протокол использует 192-битное шифрование, более устойчивое к взломам.

В итоге мы видим, что, даже при условии постоянно совершенствующихся средств защиты, улучшаются, и методы взлома, и каждый должен знать базовые принципы защиты себя и своих персональных устройств от интернет-атак.

## Список литературы

1. Широкополосные беспроводные сети передачи информации / В. М. Вишневский [и др.]. – Москва : Техносфера, 2005. – 595 с.

2. Гордейчик С. В. Безопасность беспроводных сетей / С. В. Гордейчик, В.В. Дубровин. - Москва: Горячая линия - Телеком, 2008. - 288 с.

3. Технологии современных беспроводных сетей Wi-Fi. – Режим доступа: https://okwifi.com/soveti/standarty-wifi.html. – Заглавие с экрана.

4. Стандарты Wi-Fi: список самых распространенных протоколов. – Режим доступа: https://wifigid.ru/poleznoe-i-interesnoe/standarty-wi-fi. – Заглавие с экрана.

5. Взлом беспроводной сети: способы и программы. Режим доступа: https://tproger.ru/articles/vzlom-wi-fisposoby-i-programmy/. – Заглавие с экрана.

6. Wi-Fi сети: проникновение и защита. – Режим доступа: https://habr.com/ru/post/224955/. – Заглавие с экрана.

7. Модификация метода поиска информации в сети интернет на основе использования методов индуктивного рассуждения / В. В. Лавлинский, А. Л. Савченко, И. А. Земцов, О. Г. Иванова // Моделирование систем и процессов. – 2019. – Т. 12, № 1. – С. 61-67.

## References

1. Broadband wireless information transmission networks / V.M. Vishnevsky [et al.]. - Moscow: Technosphere, 2005. – 595 p.

2. Gordeychik S.V. Security of wireless networks / S. V. Gordeychik, V. V. Dubrovin. – Moscow : Hotline-Telecom, 2008. – 288 p.

3. Technologies of modern wireless Wi-Fi networks. – URL: https://okwifi.com/soveti/standarty-wifi.html. – Title from the screen.

4. Wi-Fi standards: a list of the most common protocols. – URL: https://wifigid.ru/poleznoe-i-interesnoe/standarty-wi-fi. – Title from the screen.

5. Hacking a wireless network: methods and programs. – URL: https://tproger.ru/articles/vzlom-wi-fisposoby-i-programmy /. – Title from the screen.

6. Wi-Fi networks: penetration and protection. – URL: https://habr.com/ru/post/224955 /. – Title from the screen.

7. Modification of the method of searching for information on the Internet based on the use of inductive reasoning methods / V. V. Lavlinsky, A. L. Savchenko, I. A. Zemtsov, O. G. Ivanova // Modeling of systems and processes. – 2019. – vol. 12, No. 1. – pp. 61-67.